APPROACHES TO CYBER INTRUSION RESPONSE

A "LEGAL FOUNDATIONS" STUDY

Report 12 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00001997	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Approaches to Cyber Intrusion Response A "Legal Foundations" Study	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Presidents Commission on Critical Infrastructure Protection	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 24	

Contents

Page

Acknowledgments ..... **iii**

Preface ..... **iv**

Part One: Introduction **1**
- Research Issues 1
- Research Findings 1
- Assumptions 2
- Background 2
- Principles for Commerce on the Internet 5

Part Two: Additional Approaches to Cyber Intrusion Response **6**
- Emphasizing Increased Security Measures by Private Industry 6
- Creating an Expert Legal Study Group to Study Alternate Legal Regimes 7
- Exploration, Expansion and Use of Private Contractual or Tort Remedies 7
- Exploring Administrative Remedies 9
- Federal Licensing of Private Parties Engaged in the Business of Investigating Computer Intrusion Incidents 10
- Expanding Statutory "Right to Monitor and Detect" for Broad Range Of Users and Service Providers 12
- Developing an International Civil Enforcement Mechanism for Computer Crime Modeled on the WTO-TRIPS Intellectual Property Enforcement Mechanism 12

Part Three: Conclusions **14**

Appendices

Appendix A **A-1**

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The

series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Introduction

Research Issues

Are there viable alternatives to traditional criminal law enforcement responses (i.e., investigations, prosecutions and sanctions) that would serve as an additional deterrent to unauthorized computer intrusions?

Research Findings

- Many intrusion incidents go undetected.
- When detected, intrusion incidents are underreported to law enforcement.
- Reasons for failure to report include fear of negative publicity, fear of bestowing undue advantage to competitors, or preference for a civil remedy.
- Of the incidents reported, only a relative few result in fully successful criminal prosecutions.
- Failure of detection and under-reporting of intrusion incidents significantly dilutes potential deterrent effects of a criminal enforcement scheme.
- The limited ability of law enforcement to successfully prosecute all reported incidents significantly dilutes potential deterrent effects of a criminal enforcement scheme.

Assumptions

- The number of unauthorized intrusions will continue to grow, owing to a steady increase in the numbers of people with capability and the increased availability of intrusion tools.
- Even assuming perfect reporting of intrusion incidents, law enforcement will not be able to provide a sufficiently robust response to achieve maximum deterrence.
- Additional deterrence will be needed to thwart a growing threat.
- Deterring computer crime will reduce the cyber-based threat to critical infrastructures.

Background

Although figures vary, only a small percentage of successful computer intrusions are detected. Only a small percentage of those detected are reported to law enforcement. According to the 1997 Computer Crime and Security Study (CSI Spring 1997), only 17.87 percent of surveyed companies that experienced computer intrusions over the last 12 months reported those incidents to law enforcement. This figure is essentially unchanged from 1996 (16 percent). Among the reasons cited for not reporting intrusions to law enforcement are a fear of negative publicity, restoring advantage to competitors, or preference for a civil remedy. Whether in the interest of maintaining the confidence of their customer base or retaining control of their systems, personnel and resources, the private sector has, by and large, opted to incur the costs of intrusion incidents rather than respond through currently available law enforcement avenues.

In a very real sense, private sector victims are forced to choose between notifying law enforcement and losing public trust because of constitutional considerations that require public airing of criminal allegations.[1] (Assuming as a given that the constitutional rights afforded a criminal defendant are unlikely to be radically transformed in the foreseeable future—this conflict will not resolve itself any time soon.) Add to this the intense media interest in high technology crime, and private sector reluctance to report known criminal incidents becomes increasingly understandable.

[1] *See* Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 Computer/Law J. 265, 284 (1991).

Victims are placed in the awkward position of having to choose between cooperation and maintaining their anonymity. They must weigh, on one hand, the benefits derived through full cooperation with law enforcement (which, in most cases, amounts only to the deterrent value derived through a successful criminal prosecution, as few criminal defendants have had the ability to make restitution for damage done), against the inordinate expense incurred in supporting an investigation and the reputational harm that can result from public acknowledgment of security vulnerabilities.[2] Maintenance of public confidence as a primary business objective often militates in favor of non-reporting. It is reasonable to expect a similar calculus to apply for the owners and operators of the critical infrastructures, given the high value that they place on maintaining public trust and confidence in the reliability and continuity of their infrastructure services. This may be especially true in highly competitive industries such as commercial airlines, banking, and long-distance telecommunications, or in infrastructure sectors that are just starting to move toward competition, such as electric power.

In addition, several writers have acknowledged obstacles to the successful investigation and prosecution of computer-related offenses.[3] First there are legal obstacles. The current legal structure for prosecuting computer crimes including intrusions is fraught with difficulties ranging from proving intent to establishing jurisdiction and it may be many years until the actual laws, law enforcement personnel, and judicial systems operate in such a way that they will maximize deterrence to criminal behavior.[4]

Even assuming an ideal legal climate, practical difficulties arising from the resource-intensive nature of computer crime investigations will continue to hinder the achievement of maximum deterrence through a traditional law enforcement response. Investigations are extraordinarily resource-intensive. In terms of personnel alone, while an average "low-tech" state or local investigator may handle a normal load of 40-50 cases per month, a "high-tech" investigator can only handle 3 or 4 per month.[5] Equipment is expensive, and must be frequently improved or replaced to keep pace with the technology used by intruders. Incidental investigative costs (such as travel) remain high, owing to the multi-jurisdictional nature of the offenses. And these costs are frequently borne by more than one investigative agency that may be actively involved in investigating the same series of intrusion incidents.

Congress has been agreeable to improving laws relating to computer crime, as evidenced by amendments to the Computer Fraud and Abuse Act and the passage of the Economic Espionage Act of 1996. The Department of Justice is currently working on proposed legislation to further streamline the national and international law enforcement response.

---

[2] *Id*.

[3] *See, e.g*., Michael P. Dierks, *Computer Network Abuse*, 6 Harv. J. L. & Tech. 307 (1993); James A. Fagin, *Computer Crime: A Technology Gap*, 15 Int'l J. Comp. & Applied Crim. Justice 285 (1991); B.J. George, *Contemporary Legislation Governing Computer Crimes*, 21 Crim. L. Bull. 389 (1985).

[4] *See* Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm*, 35 Jurimetrics J. 1, 8-9 (1994).

[5] Ingrid Becker, *Cybercrime: Cops Can't Keep Up with Technobandits*, 15-Jun Cal. Law. 47, 91 (1995) (quoting Bill Spernow, SEARCH Group, Sacremento California).

Congress has now taken the first step toward the creation of a meaningful federal *civil* remedy for victims of computer crime. The 1994 amendments to the Computer Fraud and Abuse Act created a limited civil cause of action for victims to use against violators to obtain compensatory damages (limited to economic damages) or injunctive relief. The 1996 amendments to Section 1030 now make civil remedies available for any violation of Section 1030, including any of its 7 subsections (a)(1) through (a)(7). Economic damages are available for violations that cause a loss of $5,000 or more. No limitation on damages is imposed for violations that modify or impair medical treatment, examination or diagnosis, that cause or threaten physical injury, or that threaten public health or safety. This new cause of action is rarely exercised however. To date, the civil remedy has been invoked only once—unsuccessfully, by a pro se plaintiff against his former employer—in an unpublished opinion.[6]

The Administration, in its *Framework for Global Electronic Commerce*, has defined the appropriate role for government as "encourag[ing] industry self-regulation wherever appropriate and support[ing] the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet."[7] With regard specifically to electronic commerce, the Administration has registered a preference for "a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce." Fostering a more well defined and robust civil liability climate appears to be consistent with this general guidance. Toward this end, the President and Vice President have embraced efforts by a number of groups to adapt the Uniform Commercial Code and other laws to cyberspace, and the adoption of uniform legislation by all states. In the *Framework*, the President and the Vice-President set forth both broad and specific principles to guide growth of commerce on the Internet. Some of these principles may be a helpful frame of reference when thinking about alternatives to the traditional law enforcement response.

[6] *See* Letscher v. Swiss Bank Corp., No. 94 Civ. 8277 (LBS), 1996 WL 183019 (S.D.N.Y. April 16, 1996) (unpublished).

[7] Http://www.whitehouse.gov/WH/New/Commerce/read.html (July 18, 1997).

PRINCIPLES FOR COMMERCE ON THE INTERNET

- **Principles for the Global Information Infrastructure:**
  - the private sector should lead;
  - governments should recognize the unique qualities of the Internet.

- **Principles for Rules Governing Electronic Commerce:**
  - parties should be free to order the contractual relationship between themselves as they see fit;
  - rules should be technology neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future); and
  - existing rules should be modified and new rules should be adopted only as necessary or substantially desirable to support the use of electronic technologies.

It may prove productive to consider whether there may be viable alternatives to the traditional criminal law enforcement response that may counter or avoid some of the perceived shortfalls and difficulties noted in this paper. The following options are specifically designed to supplement the existing law enforcement response and will work equally well in conjunction with an enhanced law enforcement response, to the extent options are considered under the PCCIP supplemental report *Adequacy of Criminal Law and Procedure (Cyber)*. Instead of further regulating reporting of intrusions, there may be alternatives that will be more effective in garnering private sector support, participation, and, that will ultimately result in enhanced deterrence. Civil and administrative sanctions and proceedings, for example, can occur in a less public environment in comparison to criminal prosecutions, but with a proportionate loss of deterrent effect. However private sector responses are structured, issues regarding liability, maintenance of the rule of law and privacy should be addressed and balanced.

Part Two

Additional Approaches To Cyber Intrusion Response

Emphasizing Increased Security Measures by Private Industry

A strategy aimed predominantly at enhancing governmental response is by its very nature, both government-centric and reactive. There are benefits from the private sector reserving for itself a greater degree of defensive and responsive capability. Inherent in this idea is for Congress to help the private sector concentrate funding on security measures that will reduce intrusions from small-time hackers, thereby allowing more limited law enforcement resources to be spent apprehending sophisticated and dangerous computer criminals.

- **Pro:** An emphasis on increased security may prove more cost-effective for government by alleviating or externalizing some of the costs associated with the investigation and prosecution of recreational hackers. A security-based approach to minor incidents can prevent damage which reactive measures like prosecutions and civil actions may not be able to repair.

- **Con:** This option may convey to the public an impression of law enforcement complacency to computer crime, which could ultimately reduce rather than increase deterrence. Government may not be able to contribute the resources necessary to effectively raise the private sector's level of security given changes in technology over time.

Creating An Expert Study Group To Explore Alternative Legal Regimes

It is difficult to arrive at a comprehensive solution that strikes delicate balances between public and private response, and between criminal, tort, and contractual liability. The White House or Congress may consider forming an expert study group to explore supplemental response mechanisms.

- **Pro:** This approach acknowledges that a fundamental shift in controlling legal regimes must necessarily involve careful consideration of a broad range of legal alternatives, each of which must appropriately address societal concerns such as liability exposure, maintenance of the rule of law, and privacy.
- **Con:** This approach invariably delays resolution of the problem. A study group may be tempted to "wait and see" what courts do under prevailing legal regimes before developing positions.

Exploration, Expansion And Use Of Private Contractual Or Tort Remedies

The Administration can expressly recognize the value of contractual or tort remedies as applied to various "cyber relationships," and can urge Congress to enable the private sector to implement avenues through which it can pursue alternative remedies. One possibility might be to encourage Internet hosts and users to enter into binding contractual arrangements specifically setting forth one another's rights and responsibilities. The Administration might also describe and suggest the use of tort-based remedies such as trespass and invasion of privacy, or perhaps even the creation of new civil rights of action for "cyber torts." Either method or some combination will require further study to determine long-term effects of such a system as well as the proper modes of implementation.

Private, Contract-Based Approach

Under a contract-based approach, contractual agreements between Internet users would provide a basis by which to claim damages for breach of contract as a result of unauthorized access. In order to form a network of contractual relationships, users would sign agreements stating acceptable conduct in order to obtain access privileges from Internet providers. Providers would link to other sites using similar agreements. Users would have to register aliases with their providers or hosts. Providers themselves would be the first line of enforcement, as system operators would monitor systems for inappropriate actions and identify users acting in violation of their contractual agreements. Providers and sites could take action against an intruder, including notifying them of the inappropriate nature of their conduct; requiring them to submit to monitoring as a condition of continued access; or suspension or withdrawal of access privileges.[8]

- **Pro:** This approach would allow "policing" of the Internet to be done by those in the best position to monitor activities—the system operators. The scheme would be entirely consensual; all monitoring is with knowledge and consent of users. Wide acceptance of a contractually based "code of conduct" may reduce other problems related to unsolicited e-mail, indecency, or privacy violations.

- **Con:** A network of consensual relationships between authorized users would take time to develop and will be difficult to implement. Laws may have to be changed to allow for expanded monitoring by system administrators in order to enforce the system. Privacy advocates and Internet users may be reluctant to sign on to a system of involving increased monitoring. Sanctions may not be severe enough to provide adequate deterrence to a hacker who poses a serious threat. The availability of alternate channels to the Internet may nullify effectiveness and deterrent effect.

Private, Tort-Based Approach

Under an enhanced tort-based approach, substantial remedies in tort for unauthorized access to or use of computers and computer systems would provide financial deterrents to potential hackers. Such an approach is likely to take shape, in the states, out of existing causes of action for trespass or violations of privacy, or out of new civil actions specifically tailored to cyber intrusions and the potential damages they cause. As noted above, although a federal civil cause of action now exists, it is not being used. Congress may want further consideration of or modification to the civil right of action set forth at 18 U.S.C. Section 1030(g) to make it more widely available as an alternative and effective remedy.

[8] This scheme is based on a model suggested in Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm*, 35 JURIMETRICS J. 1-15 (1994).

- **Pro**: This approach allows the victim an alternate route if criminal prosecution is declined or unsuccessful. The lower standard of proof in civil matters may ease burdens on investigators and plaintiffs allowing greater success than in criminal proceedings. Monetary damages would allow a victim to be financially compensated for the harm done to their systems or businesses as a result of the unauthorized access. Injunctive relief could be used to establish limited conditions of system use for known violators.

- **Con:** The difficulty of identifying the proper defendant and collecting evidence may prevent the victim from going forward with a civil action. Current civil actions and damage awards may not provide a sufficient incentive for a victim to go forward with a costly civil action, necessitating some expansion of remedies or other change in the law (e.g., treble damage provisions, etc.). For this option to be successful in terms of deterrence, numerous cases will have to go forward with substantial damage awards which may create a burden for the court system. Publicity surrounding large damage awards may not give the victim the confidentiality that they desire.

Exploring Administrative Remedies

There may be a need for an effective "middle ground" response to supplement existing private or law enforcement response mechanisms. Such an approach may take the form of administrative remedies and enforcement mechanisms to adjudicate broad "invasions of privacy" or "trespass" claims arising from unauthorized intrusions. This enforcement regime, the equivalent of "speeding tickets in cyberspace," could include injunctive remedies and substantial fines, as well as procedures that include the use of non-disclosure provisions to promote confidentiality and avoid publicity inherent in criminal actions.

In such a regime, a body could establish "rules of the road" and an administrative enforcement mechanism would be put in place to adjudicate violations. Rules could be set by a group after appropriate public comment period, and could be designed to prohibit unauthorized access, spamming, viruses, and privacy violations. Enforcement could be carried out by local, state and federal law enforcement personnel, who would issue on-line citations for violations observed. Victims or observers of prohibited activity could file complaints with an administrative hearing board. Sanctions could include citations with fines, targeted courses on rules, suspension of privileges, etc. Law enforcement can refer to the board cases that are not appropriate for criminal prosecution.

- **Pro:** This approach allows for enforcement and application of penalties without publicity associated with criminal investigations. It allows adjudication of computer

incidents without the expense of standing up full-scale criminal investigations or engaging in a lengthy civil trial.

- **Con:** It would demand a complex regulatory enforcement mechanisms to oversee investigation and adjudication of disputes. This relatively heavy-handed, governmental type of solution may still fail to achieve widespread acceptance within the private sector. It will require considerable study and resources before implementation is possible. It would be heavily reliant on law enforcement resources to "patrol" the Internet for violations and issue citations, contrary to existing law enforcement policies and public expectations.

Federal Licensing Of Private Parties Engaged In The Business Of Investigating Computer Intrusion Incidents

The Federal government could issue professional licenses to qualified individuals engaged in the growing business of investigating computer intrusions. Under such a scheme, the FCC or other federal regulatory body would issue licenses to qualified private investigators to track and identify unauthorized intruders. The licensing body would dictate requirements for eligibility and renewal of the license, public liability, and standards of conduct.

This novel idea would have Congress look at the feasibility and advisability of Federally licensing computer security experts to track and identify unauthorized intruders. The proposal could be based extensively on the state model for licensing private investigators. The hallmarks of such licensing schemes are stringent educational requirements, training courses and on-the-job training requirements, including examinations and continuing education requirements; liability requirements in the form of bonds and/or public liability insurance; and administrative oversight of misconduct.[9]

Each of the elements of a licensing scheme would have to be carefully considered and delineated to ensure coverage is neither too broad nor too narrow and to ensure that the licensing scheme provides benefits to all interested parties—potential licensees, customers, and the government. The licensing scheme will have to be carefully placed and designed to avoid an appearance that

[9] For a proposal whereby a Federal licensing scheme for computer security expert investigators is described in more detail, *see* Stevan A. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 Harv. J. L. & Tech. 699-732 (1998). (Note: This report has been updated since the publication of the PCCIP report to refer to the "Private Intrusion Response" article.)

recipients of licenses are acting as federal agents and are subject to the same legal constraints and liability.[10] In fact, by using state laws for private investigators as a model, it may be necessary to insulate the investigator-client relationship through a statutory privilege. While these vary from state to state in terms of coverage, most states do protect clients from unauthorized disclosure of investigatory information.

Such a proposal raises related issues as to the availability of *legal* investigatory techniques in the area of computer security. Under the current statutes governing interception of electronic communications consent is an exception to the general prohibition on interception. It may be premature to determine whether consent is an adequate legal basis for any investigator to perform the necessary steps to trace the source of an intrusion. To answer this question more must be known about the types of techniques available to private investigators and the use and effectiveness of their potential customers' "banner" warnings and notifications. While some amendment to current laws may be necessary and appropriate to facilitate such investigations, and for other purposes, it is not clear at this time that the current legal framework is an impediment to such a licensing scheme.

The benefits of elevating cyber-investigation to a legitimate, sanctioned profession will include enhanced deterrence of computer-based attacks on critical infrastructures. It would likely increase successful investigations of intrusions by creating an avenue for the private sector to investigate incidents with the degree of confidentiality and control that they desire, while allowing the government to externalize costs of petty computer intrusions. The government can then concentrate resources on computer crime investigations with implications for national security. Ultimately, both avenues may lead to more successful prosecutions of cyber criminals. In the meantime, a licensing scheme would create the needed standards of professionalism and protections of privacy that are currently lacking from what is a growing, but seldom discussed line of business. The license may contribute to the open and successful growth of such businesses, providing a defined liability climate and a government stamp of approval for investigator credentials. The cadre of investigators licensed through such a program will provide valuable services not only to the private sector, but also to the government through limited reporting (e.g., investigation statistics—how many per month, types of systems, successful tracing of intruders) and a promise of availability to assist in national cyber-emergencies.

- **Pro:** This approach might enhance deterrence while promoting responsible cyber-investigation. It might help clarify the liability climate for practitioners and for those potentially damaged. Provisions could be made to assure private-sector confidentiality and control. It would allow government to externalize the costs of minor investigations and concentrate its limited resources.

- **Con:** This approach calls for an administrative mechanism for oversight. Further study will be needed into the details before implementation will be possible.

[10] For this reason, the licensing scheme should be administered by a non-law enforcement agency. It may be appropriately housed within the FCC as it is fairly congruent with its current statutory mission.

Expanding Statutory "Right To Monitor And Detect" For Broad Range Of Users And Service Providers

Currently, 18 U.S.C. Section 2511(2)(a)(i) permits electronic service providers to intercept, disclose, or use communications when it is necessary incident to the rendition of service or to protect rights or property of the service provider. Wire service providers are limited to observing or random monitoring for mechanical or service quality control checks. The Administration could recognize a need for this statute to specifically authorize system owners and operators to monitor their systems and compile evidence of intrusions, their source, and any illegal activities while in their systems for use in civil suits or by law enforcement.

- **Pro:** This approach would more clearly set forth rights and responsibilities of owners and users that is lacking in current federal legislative scheme, which is controlled by laws originally devised to govern telephonic but not computer-based communications. It may work in conjunction with other alternatives to traditional law enforcement.

- **Con:** Enforcement exceptions may, of necessity, be so broad as to authorize a wide range of activities currently prohibited by exiting legislation. This approach would likely substantially reduce expectations of privacy in otherwise unprotected communications.

Developing An International Civil Enforcement Mechanism For Computer Crime Modeled On The WTO-TRIPS Intellectual Property Enforcement Mechanism

Congress and the Administration could also actively expand the international availability of civil remedies for computer crime violations through organizations such as the World Trade

Organization. These efforts could be modeled after existing mechanisms that provide for international civil enforcement of intellectual property violations.

The World Trade Organization's (WTO) mechanism for enforcing intellectual property rights infractions is a potential model for international computer crime legal development—including civil remedy enforcement. Implemented by the WTO, a successor to the GATT, the Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires all 131 signatory countries to create and maintain minimum standards for protecting intellectual property rights; TRIPS additionally requires that all countries create legal mechanisms for adjudicating civil disputes. TRIPS sets a timetable for developing:

- law enforcement investigative procedures;
- procedural rules that are not onerous or overly complicated; and
- enforcement proceedings, whether administrative or judicial.

TRIPS permits signatory countries to develop legal and law enforcement mechanisms within the parameters of existing legal structures and institutions. TRIPS establishes a timetable for all countries to meet minimum standards. The more advanced countries offer technical assistance and training to assist lesser developed and developing signatory members. For a more detailed treatment of this issue, refer to Appendix A.

- **Pro:** The WTO-TRIPS model advances international communication and may be available to set timetables for cooperation over complex computer-related intrusions and related investigations. The model provides a framework for defining and implementing methods and goals currently used in the United States, Japan, and most European countries. The WTO-TRIPS model may be used to offer developing and lesser-developed countries incentives to implement legal mechanisms for investigating and enforcing civil judgments for computer-related intrusions. WTO-TRIPS could channel information and training in law enforcement, computer forensics, and administrative and judicial procedures to member countries. International organizations are not focusing on lesser developed or developing countries. The WTO-TRIPS model mandates National Treatment and Most-Favored-Nation benefits for law enforcement investigations; additionally, WTO-TRIPS mandates similar treatment for judicial proceedings and civil penalty enforcement.

- **Con:** Potentially tenuous connection between world trade and computer abuse may cause skepticism among member countries. Implementing the agenda will require a tremendous amount of time and effort. Numerous other international organizations are addressing issues associated with computer-related crime, including the P8/G7, EU, OECD, and the United Nations. There is little if no support for an additional international organization to focus on computer crime enforcement.

Part Three

Conclusions

Traditionally, law enforcement investigations and prosecutions have been seen as the principal source of deterrence for criminal activity. However, based on what appears to be a growing trend toward private "security" services ($6 billion in 1996), and the unique nature of computer intrusions, there some day may be a need to supplement law enforcement deterrence. While there are many possible supplements to a traditional law enforcement response, all of the options considered have one thing in common—they place the control of the investigation and prosecution and their costs in the hands of the victim.

Appendix A

WTO Intellectual Property Enforcement Mechanism

Existing international organizations and agreements offer mechanisms for enforcing civil penalties associated with computer-related crimes. These agreements also present an excellent model for providing training and technical assistance to countries to adopt and enforce substantive and procedural standards for computer-related crimes.

One particular model might be the agreements negotiated and implemented by the General Agreement on Tariffs and Trade (the "GATT"), and its successor organization, the World Trade Organization ("WTO").[1]

The TRIPS agreement is recognized by all 131 signatory countries and mandates legal protection for intellectual property rights and enforcement mechanisms.[2] TRIPS includes highly-negotiated and extensive provisions for enforcing a final decision – including a dispute resolution mechanism. TRIPS also creates responsibilities for more advanced countries to offer technical assistance and training to lesser developed signatory countries.

Flexibility

TRIPS is a minimum standards agreement, which allows members to provide more extensive protection. The agreement also permits signatories to determine the appropriate method of implementation in the context of their own legal system and practices.

[1] The WTO is an inter-governmental organization resulting from the GATT Uruguay Round negotiations (1986-1994). The WTO adopted the GATT agreement in addition to other agreements from the Uruguay Round talks – including the General Agreement in Trade and Services ("GATS") and, more importantly, the Agreement on Trade-Related Aspects of Intellectual Property ("TRIPS").

[2] The WTO's purpose is to facilitate trade flow as smoothly as possible in a system based on rules, to settle trade disputes between governments, and to organize trade negotiations. In May, 1997 WTO membership included 131 countries. For more background information, please refer to the WTO's Web Site at http://www.wto.org/.

Enforcing Judgments

TRIPS allows for differences in various legal regimes, but mandates specific *minimum standards* and *general principles* that all signatory enforcement regimes must incorporate, including civil and administrative remedies, special requirements for criminal sanctions, and procedures and remedies available so right holders may effectively enforce their rights.[3]

The following summarizes TRIPS' specific obligations for enforcing civil judgments:

General Obligations

TRIPS mandates clear and transparent general requirements, and include:

- rights to expeditious process of claims and remedies;
- construction of legal and administrative deterrents to breaches of law;
- rights to enforcement procedures that are not costly or complicated;
- rights to judicial and administrative appeal;
- obligations to create mechanisms to facilitate legal transparency.

Civil and Administrative Procedures and Remedies

TRIPS outlines in great detail the minimum standards and basic features for civil judicial procedures. Particulars include minimum standards for application of:

- basic rules of evidence;
- due process (*e.g.*, written notice, expeditious remedy, and complaint with sufficient detail);
- court or administrative body's right to seek production of evidence;

[3] The general enforcement provisions are in Part III of TRIPS.

- court or administrative body's right to punish an uncooperative party;
- safeguards for abuse of judicial or administrative power; and
- application of criminal sanctions for certain willful violations.

National Treatment and Most Favored Nation Treatment

All WTO Members must provide *National Treatment* and *Most-Favored-Nation-Treatment* ("*MFN*") to all other Signatories under TRIPS.[4] National Treatment means that a Member country must afford to foreign nationals (from Member countries) all protections and access to enforcement mechanisms no less favorable than it accords to its own nationals. MFN awards "any advantage, favor, privilege and immunity granted by a Member to the nationals of any other country."[5] This would include:

- law enforcement arrangements;
- judicial assistance in capturing perpetrators; and
- administrative or judicial assistance in enforcing civil penalties.

With regard to judicial and law enforcement assistance, both National Treatment and MFN could facilitate investigations of computer crimes. Further, these legal regimes would create incentives for all countries to develop legal mechanisms to enforce civil penalties arising from computer-related crimes.

Dispute Settlement

The TRIPS agreement makes disputes over obligations subject to the WTO's dispute settlement procedures.[6] The Dispute Settlement Body ("DSB") has exclusive jurisdiction to implement the dispute settlement process. TRIPS sets forth a process to form DSB panels for mediation and arbitration. TRIPS also allows for appeals to the WTO from DSB panel final decisions. The DSB enforces all decisions and maintains surveillance over the decision implementation process.

[4] TRIPS Agreement, Articles 3 (National Treatment) 4 (MFN Treatment).
[5] TRIPS, Article 4.
[6] TRIPS, Article 64.

Transitional Arrangements - Obligations Created

TRIPS gives all WTO members transitional periods so that they can meet their obligations. Transitional periods depend on the level of signatory-country legal and economic development.[7] In all cases, however, signatories are not permitted to "back-slide." All lesser-developed countries are expected to implement TRIPS within set periods of time.[8]

TRIPS additionally imposes affirmative obligations on developed countries to train and assist lesser-developed countries to meet time deadlines to implement various requirements.[9] Such technical assistance includes assistance in preparing laws and regulations, systems to prevent judicial and administrative abuse of power, and training for officials involved in enforcement of legal authorities and mechanisms.

TRIPS also includes a general agreement by all members to cooperate in general enforcement of TRIPS. This includes greater communication, establishment of contact points, and promotion of exchanges in cooperation and communication.[10]

Summary of a Dispute Within the WTO-TRIPS Legal Regime

The Dispute

1. Dispute arises; party may seek redress within Member country legal system. Under WTO-TRIPS, all Member countries must afford National Treatment ("no less favorable than it accords its own nationals…") and Most-Favored-Nation-Treatment ("… any advantage favor, privilege or immunity granted by a Member to the nationals of any other country…").

[7] TRIPS, Articles 65-66.
[8] For example, so-called developing countries have five years to implement TRIPS.
[9] TRIPS, Article 67.
[10] TRIPS, Article 69.

2. Violating Country must afford to other Member country judicial and law enforcement assistance consistent with benefits for its own nationals.

3. WTO will expect parties to attempt settlement bilaterally;

4. If this fails, WTO, in strict accordance with TRIPS, invites parties to seek assistance from the WTO Director-General – acting in an *ex officio* capacity seeks to mediate dispute;

5. If consultations fail to arrive at a solution after 60 days, complainant may ask the Dispute Settlement Board to establish a "Panel"; the establishment of a Panel is almost automatic;

6. The Panel's procedures are set forth clearly in TRIPS and require the Panel to assist the DSB in making its decision in light of the existing documents;

7. The Panel, after hearing the matter, drafts a Report; the DSB must then "adopt" the Report;

8. Once adopted, either party may appeal to the Appellate Body, which can then modify the Report;

Implementation and Enforcement of Remedy

1. According to TRIPS, parties are expected to adhere promptly to all DRB/Appellate Body decisions.

2. TRIPS instructs parties to report, within 30 days of the decision, their intentions with regard to the decision;

3. If impractical to comply immediately, DSB provides a "reasonable period of time" to comply;

4. After this period, if the party has still not complied, the losing party is instructed to negotiate on a mutually accepted compensation;

5. If the parties cannot come to agreement, the DSB may suspend certain concessions that the losing party may enjoy under TRIPS.

6. DSB monitors compliance.